
# Maryland Cloud Services Security Policy

**Last Updated:** 06/09/2017

# Contents

## 1.0 Purpose

Organizations are increasingly moving infrastructure and operations to hosted providers in order to provide data and tools to employees efficiently and cost-effectively. The security posture of **Cloud Service Providers (CSP)** must be adequately assessed and meet minimum security requirements before any State of Maryland information, system, or infrastructure can be hosted outside of a State-managed environment.

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. This includes ensuring that cloud environments hosting State of Maryland Executive Agencies meet specified security controls and do not endanger the security posture of the State.

The Maryland Department of Information Technology (DoIT) will utilize the baseline controls and standards established by NIST Special Publication (SP) 800-53R4, SP 800-144, SP 800-145, and SP 800-146 guidelines to develop this policy.

## 2.0 Document and Review History

This policy supersedes the State of Maryland Information Security Policy (version 3.1, Feb 2013) Section 9: Cloud Computing Technologies and any related policy regarding hosted application and cloud computing declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

| Date | Version | Policy Updates | Approved By: |
|---|---|---|---|
| 01/31/2017 | v1.0 | Approval of Draft | Maryland CISO |
| 06/09/2017 | v1.1 | Initial Publication | Maryland CISO |

## 3.0 Applicability and Audience

This policy is applicable to all agencies supported by, or under the policy authority of, the Maryland Department of Information Technology, including contractors, vendors, and agents of such agencies that are involved with hosting services. DoIT will be responsible for enforcing the security of cloud environments in accordance with the requirements in this policy for all agencies that are Enterprise onboarded.

Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy when using a cloud service provider to host State data or any operational function.

## 4.0 Policy

When multiple organizations use a single CSP, organizations can benefit from an economy of scale. However, using a CSP centralizes management of information and applications as data and processing are shifted out of the direct control of formerly distinct IT and security groups. When utilizing a shared CSP, security teams must institute a set of (CSP and operational) controls as

directed in this policy to govern and mitigate risks, ensuring the safety of State data, operations, and IT resources.

Cloud computing solutions used by the State of Maryland Executive Branch agencies must have the configuration, deployment, and management structures than can meet the State's security, privacy, and other requirements.

## 4.1 Preliminary Requirements

All cloud providers utilized by the State of Maryland Executive Branch systems must meet the minimum requirements outlined below.

| # | Name | Requirement |
|---|---|---|
| A | Compliance with State Cybersecurity Standards | Cloud providers must be able to comply with requirements as established within the Cybersecurity Program Policy and all supporting policies, including this document. |
| B | Agency Authorization | Agencies seeking to use cloud services must submit a System Security Plan (SSP) and receive an Authority to Operate (ATO) or an Interim Authority to Operate (IATO) signed by their respective Designated Authority (DA) before data or applications can be hosted on a cloud service provider. See *Security Assessment Policy* and *Cybersecurity Authority to Operate Policy.* |
| C | Classification of Data | Agencies must anticipate and mitigate risks of cloud-hosted data and resources in accordance with the *DoIT Asset Management Policy*, Data Classification Guidelines. |
| D | Agency Accountability | Agencies are considered data owners and are responsible for ensuring the security of the data and any operational functionality the agencies choose to host externally.<br><br>NOTE: In the event of a cloud provider experiencing a data breach, data owners are still responsible and accountable for protecting State confidential information and must ensure SLAs and State contracts enforce culpability across all parties. |
| E | Geographic Limitations | ▪ Network administrators who have high-level access privileges are prohibited from accessing cloud network resources to make changes from outside of the continental United States<br>▪ All data and State services must be hosted on servers located within the continental United States, preferably in the same region as the State. |

## 4.2 Vendor Assessment

Agencies will assess a CSP and ensure the CSP can operate in accordance with the requirements outlined below.

| # | Name | Requirement |
|---|---|---|
| A | Assess Competency of Provider | Agency must exercise due care and due diligence and conduct a thorough analysis of the provider's capabilities and security measures. This can be done through: |

| # | Name | Requirement |
|---|---|---|
| | | ▪ Detailed questionnaire given to the CSP<br>▪ Research into the company<br>▪ External vendor-assessment reports or audit results<br>▪ Previous client testimonials<br>▪ Vendor-provided **FedRAMP** certification, if compliant |
| B | Establish Contractual Obligations | ▪ CSPs may have standard contractual language; to the extent possible, an agency must negotiate with the provider to contractually include required protections described within Sections 4.3 and 4.4 of this policy, if not already covered in the standard contractual language<br>▪ Contracts should be re-evaluated upon any change to the CSP as a third-party entity (e.g., bought by another company, bankruptcy); CSP standard contract language; or revisions to the terms and conditions of provided services and products |
| C | Continuous Assessment | ▪ CSPs must agree to ongoing evaluation by the contracting agency to ensure that security measures are properly implemented and enforced<br>▪ Any violation of security measures affecting the security of State information or resources must be addressed and remediated as soon as possible after discovery |
| D | Regulatory Compliance | CSPs should demonstrate compliance with regulatory requirements as applicable: PCI DSS, HIPAA, FedRAMP, **CSA**, **SSAE16** (SOC1-financial, SOC2-IT controls, SOC3-attestation), or **ISO**. |

## 4.3 Privacy and Security Controls for Cloud Hosting

Agencies must verify that potential cloud service providers, at minimum, have or can provide the capabilities and functionalities outlined below.

| # | Name | Requirement |
|---|---|---|
| A | Electronic Discovery | Ensure that cloud provider's electronic discovery capabilities, processes, and policies do not compromise the privacy and security of data and applications. |
| B | Continuous Monitoring | Ensure hosted systems or services are capable of supporting agency continuous monitoring as a security functionality and can provide data reports to management for security and risk assessments. |
| C | Architecture | Understand the underlying technologies that the cloud providers use to provision services and how that integrates with current (agency) structure. |
| D | Identity and Access Management | Ensure adequate safeguards are in place to secure authentication, authorization, and other identity and access-management functions in accordance with the requirements outlined in the *DoIT Data Security Policy.* |
| E | Software and Data Isolation | CSP must show, in multi-tenant offerings, that the structure or architecture of the provider isolates hosted data and operations from other tenants so the agency can accurately assess potential risks for its "independent" tenancy. |
| F | Availability | Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations will be reestablished within an agreed-upon time. |

| # | Name | Requirement |
|---|---|---|
| G | Incident Response | ▪ Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident<br>▪ Ensure that agency and CSP staff can easily and directly coordinate response efforts to incidents in accordance with the respective roles and responsibilities for the operational environment<br>▪ Ensure that the cloud provider informs the agency within a reasonable time after a breach has been discovered that directly impacts the agency resources or data. |

## 4.4 Service Level Agreement (SLA) Requirements

It is imperative for agencies to establish SLAs that clearly delineate rights and responsibilities between the agency and the cloud service provider. At minimum, SLAs should include a description of, and agreement on, the matters outlined below.

| # | Name | Requirement |
|---|---|---|
| A | Full set of Terms and Conditions | Agencies should have a full set of Terms and Conditions documentation from a cloud service provider, including, but not limited to:<br>▪ SLA<br>▪ Privacy Policy<br>▪ Acceptable Use Agreement |
| B | Data Location Limitations | SLA should limit the geographic location of data storage to the continental United States, and, whenever possible, the East Coast. |
| C | Data Ownership | ▪ Data ownership will remain with the Agency at all times<br>▪ Each agency must define what data affected by the agreement is considered "confidential" under MD law, and, as feasible, specify appropriate security |
| D | Visibility into Security Measures | Agencies shall have visibility into the security measures of the CSP to manage risk and audit security status of their data and resources. |
| E | Access Limitations | CSP must be able to employ, or allow the agency to employ, access controls to prevent unauthorized access to agency data and information resources affected by the agreement. |
| F | Cryptographic Key Management | The agency will control cryptographic key management and auditing, not the CSP. |
| G | Data Sanitization | Stipulations on data sanitization should include measures to ensure CSP-held data is sanitized appropriately, either at agency request or when an agency withdraws from the service. |

# 5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

## 6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Cybersecurity Authority to Operate Policy
- Data Security Policy
- Security Assessment Policy

## 7.0 Definitions

| Term | Definition |
|---|---|
| **Cloud Security Alliance (CSA)** | Third party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001 management system standard together with the CSA Cloud Controls Matrix, a specified set of criteria that measures the capability levels of the cloud service. |
| **Cloud Service Provider (CSP)** | A company that offers some component of cloud computing — typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) — to other businesses or individuals. |
| **Federal Risk and Authorization Management Program (FedRAMP)** | Federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. |
| **International Organization for Standardization (ISO)** | An international standard-setting body composed of representatives from various national standards organizations which promotes proprietary, industrial, and commercial standards. |
| **Standards for Attestation Engagements No. 16 (SSAE16)** | Auditing standard for service organizations, often used to report compliance with Sarbanes Oxley Act. |

## 8.0 Enforcement

The Maryland Department of Information Technology is responsible for enforcing policies for Enterprise onboarded agencies. The DoIT Cybersecurity Program identifies the minimum requirements necessary to comply with the information security standards and guidelines provided within Cyber Security Program Policy and its supporting policies. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize DoIT to limit or restrict an agency's access to external and internal communications (effectively shutting down connectivity) until the agency becomes compliant.

Cloud environments found to be in operation without an ATO or IATO, or found to be in violation of the terms under which the ATO or IATO were granted, may be subject to immediate deactivation or disconnect from other agency environments and third parties.

Any personnel found to have violated this policy will be subject to investigation and possible disciplinary action, which may include written reprimand, suspension, termination, and possible criminal and/or civil penalties.